

25 JANUARY 1999



Operations

**CONTROL OF SINGLE INTEGRATED
OPERATIONAL PLAN (SIOP)- EXTREMELY
SENSITIVE INFORMATION (ESI) ACCESS**

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the Malmstrom Electronic Publication Distribution Library (MEPDL) WWW site at: <http://www.malmstrom.af.mil/pdo/pubs.html> If you lack access, contact your Publishing Distribution Office (PDO).

OPR: 341 OSS/OSKEX
(Capt Matthew M. Joy)
Supersedes MAFBI 10-1101, 17 Jul 95

Certified by: 341 OG/CC
(Col Kimber L. McKenzie)

Pages: 7

Distribution: FX (HQ AFSPC/DOMN, 150
Vandenberg Street, Suite 1105, Peterson AFB CO
809141, 20 AF/DOME, 6610 Headquarters
Drive, F.E. Warren AFB WY 82005-3943.
.....1)

This instruction implements CJCSI 3231.01, *Safeguarding the Single Integrated Operational Plan (SIOP)*, and AFD 10-11, *Operations Security*, and establishes procedures for controlling access to SIOP materials. This instruction is consistent with guidance provided in AFI 10-1102, *Safeguarding the Single Integrated Operational Plan (SIOP)*. It applies to all personnel assigned to the 341st Space Wing and subordinate units, and personnel assigned or attached to, or supported by, Malmstrom AFB.

This publication requires collection and or maintenance of information protected by the Privacy Act of 1974. The authorities to collect and or maintain the records prescribed in this publication are U.S.C. 8013 Secretary of the Air Force and or Executive Orders 9397, 9838, 10450, and 11652. Forms affected by the Privacy Act have an appropriate Privacy Act Statement. System of records notice F205 AFSCO C, *Personnel Security Clearance and Investigation Records*, applies.

SUMMARY OF REVISIONS

This revision changes the Wing's designations of the 341st Missile Wing to 341st Space Wing and the Security Forces from 341 SPS/SPAI to 341 SFS/SFAI throughout, changes the individual responsible for the control and maintenance of the 341 SW SIOP account (paragraph 1.), and deletes HQ AFSPC requirement of certifying official (paragraph 2.1.9.) A (|) indicates revisions from the previous edition.

1. Responsibilities. The 341 OSS/CC is responsible to the 341 OG/CC for the control and maintenance of the 341 SW SIOP account. The Chief, Weapons and Tactics EWO Section (341 OSS/OSKE) is the individual within the 341 OSS responsible for these tasks. Commanders and staff agency chiefs are

responsible for ensuring unit security managers promptly complete AF Form 2583, **Request for Personnel Security Action**, and AF Form 2587, **Security Termination Statement**, on unit personnel.

2. Access Granting Procedures. An individual receives access to SIOP-ESI material only after 341 OSS/OSKE receives and completely processes an AF Form 2583 (see [Attachment 2](#) for an example).

2.1. An AF Form 2583 must be on file at 341 OSS/OSKE for each individual assigned to the 341 SW requiring access to SIOP material. 341 OSS/OSKE will produce and maintain a 341 SW SIOP access roster based on information provided by squadrons and staff agencies via AF Forms 2583 and 2587. The unit SIOP Representative or Security Manager will complete an AF Form 2583 on all individuals requiring SIOP-ESI access (see example at [Attachment 2](#)). Coordinate with losing Security Manager or 341 SFS/SFAI to verify clearance dates or use a current Automated Security Clearance Approval System (ASCAS) roster, if available.

2.1.1. Block 1 -- Enter individual's full name (including full middle name).

2.1.2. Block 2 -- Enter unit name. For the 341 OG, enter "341 OG (UNIT)," where unit is 10 MS, 12 MS, etc. This will allow the individual to move throughout the Operations Group, yet shows who filled out the original form.

2.1.3. Block 3 -- Enter rank (CAPTAIN, MAJOR, etc.).

2.1.4. Block 5 -- Verify citizenship via ASCAS roster or 341 SFS/SFAI.

2.1.5. Block 6 -- Enter DD-MMM-YY format.

2.1.6. Block 7 -- City, State, Country (Do not forget country).

2.1.7. Block 8 -- X in SBI, FINAL CLEARANCE, TOP SECRET, SPECIAL ACCESS, UNESCORTED ENTRY, PRIORITY A and type SIOP-ESI in the SPECIAL ACCESS block, as required. This is a typical example, but you may need to X different blocks if the person does not have a final clearance or does not have unescorted access (i.e., has had access to unauthorized launch studies). Mark the SBI block to show the SBI/SSBI accomplished. If the person has an SSBI, mark out the "Special Background Investigation (SBI)" and insert "SSBI" in the blank space to the right of it. Mark FINAL CLEARANCE and TOP SECRET to show the person is in possession of a final Top Secret security clearance. NO ONE WITH AN INTERIM TOP SECRET CLEARANCE WILL BE GRANTED ACCESS TO SIOP-ESI INFORMATION. Mark SPECIAL ACCESS and type "SIOP-ESI" to show this AF Form 2583 is being used for access to a special program, not requesting an investigation of some type. Mark UNESCORTED ENTRY so that the individual is eligible for a line badge. Pass and ID, 341 SFS/SFRA, will not issue a line badge unless the unit requests one using an AF Form 2586, **Unescorted Entry Authorization Certificate** (e.g., Battle Staff Advisor, etc.). This allows an individual access to SIOP-ESI information in a Restricted Area (e.g., the Command Post). Mark PRIORITY A because the individual has access to SIOP-ESI information in areas such as a Launch Control Center (LCC) or the Command Post which are Priority A areas.

2.1.8. In Part VI, mark the SIOP-ESI CONTINUING block to show a continuous need for access to SIOP-ESI. For a one-time access, consult 341 OSS/OSKE.

2.1.9. Leave Blocks 27 through 28 blank (since we do not know in advance who will sign the forms). 341 OSS/OSKE will type the certifying official's name, grade, and title. 341 OSS/OSKE will date the form in Block 27 or ensure the certifying official dates it.

2.1.10. In Part VII, enter the date and type (e.g., SBI, SSBI, SBI-PR, etc.) of the person's Top Secret Clearance, the date of their investigation, what categories they have access to, the fact that the individual received a briefing, and Unfavorable Information File (UIF) information. This information is available from an ASCAS roster or 341 SFS/SFAI. **Remember that the SIOP-ESI category numbers by themselves are unclassified, but the definitions of what the category numbers mean are CONFIDENTIAL.** THE INDIVIDUAL MUST SIGN AFTER THE LINE STATING HE OR SHE HAS RECEIVED A BRIEFING. An example remarks block follows:

TOP SECRET: YYMMDD

(May be "DCID 1/14")

SBI: YYMMDD

(May be "SSBI")

SIOP-ESI CATEGORIES 6 AND 10

INDIVIDUAL BRIEFED IAW DOD5200.1R/AFI31-401, & CJCSI3231.01. _____

NO UIF.

The individual must sign after the briefing line to verify receipt of the SIOP-ESI Access Briefing before forwarding the form to 341 OSS/OSKE. If you do not know what to brief them on, contact 341 OSS/OSKE SIOP-ESI Program Manager for a copy of the briefing. The briefing is UNCLASSIFIED. In the interest of standardization, all forms should comply with the example attached to this instruction. More information may appear in the remarks section, but the example shows the minimum required information.

2.2. Take the form to 341 OSS/OSKE. The SIOP-ESI Program Manager will ensure the form is correct and route the form through to the access granting authority for signature. Please do not take the form directly to the access granting authority. The SIOP-ESI Program Manager will check all forms for completeness before presenting them for approval and signature. This greatly reduces the amount of administrative errors requiring reaccomplishment of forms.

NOTE: An individual does not have SIOP access until the granting authority signs the AF Form 2583.

2.3. 341 OSS/OSKE will file the original, signed AF Form 2583. The squadron representative will then come to 341 OSS/OSKE, pick up a copy, and file it as required. Squadron representatives may request the copy of the AF 2583 be sent through distribution.

3. Access Terminating Procedures. When an individual no longer requires SIOP-ESI access, the unit security manager must terminate it immediately.

3.1. The unit security manager or commander completes an AF Form 2587 showing terminated access or accesses (see [Attachment 3](#) for an example).

3.1.1. To terminate access to a category of SIOP-ESI access, enter "SIOP-ESI CATEGORY X" on the "termination for access to" line. Show multiple categories with "SIOP-ESI CATEGORIES X and Y."

3.1.2. The individual strikes out the appropriate word or words on line 5 and initials in the left margin by line 5.

3.1.3. Date the form with the current date (from this point forward, the individual no longer has access).

3.1.4. Type name and organization of the person being debriefed, and the name of the debriefer.

3.1.5. Both individuals sign the form.

3.2. The individual's unit security manager files the original signed form IAW current security directives. Immediately forward a copy to 341 OSS/OSKE who will remove the individual from the master SIOP-ESI roster.

4. "For Cause" Reports. "For Cause" reports are used in obtaining permission to proceed in court-martial, administrative discharges, and civilian removal actions. Unit commanders or staff agency chiefs contemplating involuntary separation under AFI 36-3208, *Administrative Separation for Airmen*, AFI 36-3207, *Separating Commissioned Officers*, court-martial or administrative action against military members or civilian employees that could lead to a discharge or removal must first obtain permission to proceed when the member or civilian holds a special access (e.g., SIOP-ESI).

4.1. You must first get permission to proceed from the SIOP-ESI granting authority. In accordance with AFI 10-1102, the SIOP-ESI granting authority (e.g., Wing Commander) makes the decision whether or not to proceed. Do not take action on personnel who now hold or have held special access to SIOP-ESI information within the past 2 years without first obtaining this permission.

4.2. The most difficult aspect of this requirement is determining if the individual had access prior to arriving at your unit. For example, at a previous unit or base, a person may have had accesses he or she does not have in your unit. **The only way to make sure is to contact the security manager at all of the individual's current and past units.**

4.3. AFI 31-501, *Personnel Security Management Program*, chapter 8 contains further information and the required items in the report.

4.4. Contact the Wing SIOP-ESI Special Program Manager at 341 OSS/OSKE for format of the report. After units provide 341 OSS/OSKE with the required information, OSKE will coordinate, obtain approval/disapproval for, and distribute the report as required to HQ AFSPC and HQ USAF.

J. GREGORY PAVLOVICH, Colonel, USAF
Commander

Attachment 1

GLOSSARY OF ABBREVIATIONS AND ACRONYMS

Abbreviations

ASCAS—Automated Security Clearance Approval System

CJCSI—Chairman of the Joint Chiefs of Staff Instruction

DCID 1/14—Alternate ASCAS symbol for a Top Secret clearance

ESI—Extremely Sensitive Information

LCC—Launch Control Center

SBI—Special Background Investigation

SBI-PR—Special Background Investigation - Periodic Reinvestigation

SSBI—Single Scope Background Investigation

SIOP—Single Integrated Operational Plan

UIF—Unfavorable Information File

Attachment 2

AF FORM 2583 EXAMPLE

REQUEST FOR PERSONNEL SECURITY ACTION			
<small>AUTHORITY: 10 U.S.C. 8012; 44 U.S.C. 3101; and EO 8397. PRINCIPAL PURPOSES: To identify investigation, security clearance, unescorted entry requirements, and special access program authorizations. ROUTINE USES: To request personnel security investigations, record emergency or limited access authorization, entry to restricted areas, and to record special access program authorizations. SSN is used for positive identification of the individual and records. DISCLOSURE IS VOLUNTARY: Failure to information and SSN could result in assignment to less sensitive duties.</small>			
I. IDENTIFYING INFORMATION			
1. NAME (Last, First, Middle, Maiden)		2. ORGANIZATION OR FIRM SPONSOR	
Jones, Mary Beth, Smith		341 OG (341 OSS)	
3. GRADE	4. SSN	5. CITIZENSHIP	
1Lt	123-45-6789	<input checked="" type="checkbox"/> US CITIZEN <input type="checkbox"/> IMMIGRANT ALIEN <input type="checkbox"/> NON-US NATIONAL	
6. DATE OF BIRTH	7. PLACE OF BIRTH (City, State, and Country)		
1 Jan 70	Missileville, MT, USA		
II. INVESTIGATION, CLEARANCE, ELIGIBILITY, ENTRY AND ACCESS REQUIREMENTS			
8. INVESTIGATION REQUIREMENT		9. CLEARANCE, ENTRY OR ACCESS REQUIREMENT	
<input type="checkbox"/> NATIONAL AGENCY CHECK (NAC) <input type="checkbox"/> NATIONAL AGENCY CHECK-WRITTEN INQUIRIES (NACI) <input type="checkbox"/> BACKGROUND INVESTIGATION (BI) <input checked="" type="checkbox"/> SPECIAL BACKGROUND INVESTIGATION (SBI) (SSN)		<input type="checkbox"/> ONE-TIME ACCESS <input type="checkbox"/> INITIAL CLEARANCE <input checked="" type="checkbox"/> FINAL CLEARANCE <input checked="" type="checkbox"/> TOP SECRET <input type="checkbox"/> SECRET <input type="checkbox"/> CONFIDENTIAL	
<input type="checkbox"/> BI PERIODIC REINVESTIGATION (PR) <input type="checkbox"/> SBI PERIODIC REINVESTIGATION (PR)		<input checked="" type="checkbox"/> LIMITED ACCESS <input checked="" type="checkbox"/> SPECIAL ACCESS (SIOP-ESI) <input checked="" type="checkbox"/> UNESCORTED ENTRY <input type="checkbox"/> PRIORITY A <input type="checkbox"/> PRIORITY B <input type="checkbox"/> PRIORITY C	
III. LOCAL FILES CHECK			
10. TO		11. FROM	
12. DATE	13. TYPED NAME, GRADE AND TITLE OF REQUESTER		14. SIGNATURE
IV. MEDICAL RECORDS CHECK			
15. I CERTIFY a medical records check required by DOD 5200.20/AFR 205-32, has been completed and no information exists, unless shown in Section VII, which would preclude the granting of a security clearance, unescorted entry to restricted areas, or access to special program classified information.			
16. DATE	17. TYPED NAME AND GRADE OF BASE DIP SERVICES		18. SIGNATURE
V. SECURITY POLICE RECORDS CHECK			
19. I CERTIFY a security police records check required by DOD 5200.20/AFR 205-32, has been completed and no information exists, unless shown in Section VII, which would preclude the granting of a security clearance, unescorted entry to restricted areas, or access to special program classified information.			
20. DATE	21. TYPED NAME AND GRADE OF OFFICIAL		22. SIGNATURE
VI. ACCESS AUTHORIZATION			
<input type="checkbox"/> ONE-TIME ACCESS <input type="checkbox"/> LIMITED ACCESS		<input type="checkbox"/> CONTINUING <input type="checkbox"/> ONE-TIME	
23. I CERTIFY the named individual requires access to the above special program(s), meets all investigation and clearance requirements, and has been limited on program response history as outlined in the governing directive. If applicable, emergency or limited access is necessary and will not endanger the national security.			
24. DATE	25. TYPED NAME, GRADE AND TITLE OF APPROVING AUTHORITY		26. SIGNATURE
27. DATE	28. TYPED NAME, GRADE AND TITLE OF SPECIAL ACCESS PROGRAM CERTIFYING OFFICIAL		29. SIGNATURE
VII. REMARKS			
30. (If more space is needed, use reverse and show item number being continued) DCID 1/14: YYMMDD SSBI: YYMMDD SIOP-ESI CATEGORIES 6 and 10 Individual briefed IAW DOD 5200.1R, AFI 31-401, and CJCSI 3231.01 No UIF			

Attachment 3

AF FORM 2587 EXAMPLE

SECURITY TERMINATION STATEMENT

I am aware of my termination for access to *****SIOP-ESI CATEGORIES 6 AND 10***** . . .
 (Enter special access being terminated, for example, "NATO Secret," or "SIOP-ESI," or enter special access being terminated and "classified information" if both are being terminated at the same time; otherwise, enter "classified information.") I acknowledge:

1. I have read and understand the below provisions of the Espionage Act (18 U.S.C. 793, 794), the Atomic Energy Act (42 U.S.C. 2274-2277), and the Subversive Activities Control Act of 1950, as amended (50 U.S.C. 783). I understand that any unauthorized disclosure of information affecting the national defense is prohibited and punishable by law.
2. I do not have in my possession or control any documents or material of a classified nature.
3. I shall not knowingly or willfully divulge, reveal, or transmit classified information orally or in writing or by any other means, to any unauthorized person or agency.
4. I shall report to the Federal Bureau of Investigation, to a security office of the Department of Defense, or to a security office of a U.S. Embassy or Consulate, without delay, any attempt made by an unauthorized person to solicit or obtain classified information.

235. I have, ~~have not~~ (Strike out inappropriate word or words) received an oral security briefing.

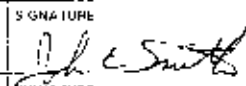
ESPIONAGE ACT AND OTHER CRIMINAL STATUTES

Sections 793 and 794 of Title 18, U.S. Code, Section 783 and 2277 of Title 42, U.S. Code, identify and prescribe punishment for certain acts which one has reason to believe will injure the United States.

50, U.S. Code, and Sections 2274, 2275, 2276 and 2277 of Title 42, U.S. Code, identify and prescribe punishment for certain acts which one has reason to believe will injure the United States.

1. Gathering, transmitting, delivering, or *Restricted Data* to an unauthorized person; information relating to national defense (including *Restricted Data*).
2. Losing information relating to the national defense through negligence;
3. Failing to report to superiors the receipt or possession of information relating to national defense;
4. Communicating classified information to an agent or representative of a foreign government;
5. Failing to deliver on demand documents or information relating to the national defense to an officer or employee of the United States who is entitled to receive it; and
6. Gathering or delivering information relating to the national defense to a foreign government.

You have had access to information relating to the national defense (including *Restricted Data*) which is protected by these statutes. These statutes make it a crime to unlawfully communicate information relating to the national defense to any person when there is reason to believe that the information will be used to the injury of the United States or to the advantage of a foreign government. The penalties prescribed for violations of these statutes, through willful acts or gross negligence, vary according to the statute, the circumstances, and the information involved. They range in severity from a fine of not more than \$2,500 to life imprisonment or death. Your signature on this form is your acknowledgement that you have been informed of the criminal statutes applicable to espionage and the punishments provided for violation of these statutes. The full text of the applicable section of each of these statutes is available for your review prior to signing this termination statement.

DATE 12 Aug 97	TYPED OR PRINTED NAME & ORGAN OF PERSON BEING DEBRIEFED John E. Smith, Capt, USAF 341 OSS/OSKC	SIGNATURE 
DATE 12 Aug 97	TYPED OR PRINTED NAME OF DEBRIEFER Bill E. Johnson, Capt, USAF 341 OSS/OSKC Security Manager	SIGNATURE 